COTS Panel

Panel Members:

Warren Naylor	BAE Systems
John Covan, PhD	Sandia National Labs.
Mike Brown	NSWCDD Code G71
Ron Stroup	FAA AIO 200
Uma Ferrell	FAA Consulting

Defining COTS

- COTS products encompass a wide variety of general-purpose off-the-shelf products (HW or SW), Non Developmental Items (NDI) and Previously Developed Software (PDS).

Note: Some of these products are designed to be user selectable/modifiable (e.g., a compiler). Vendor supplied modifications or selectables are still considered COTS. However, it must be understood that once a program modifies or enhances COTS software to meet their respective system requirements, then the modified COTS must be considered application code, subject to all certification requirements, without exception.

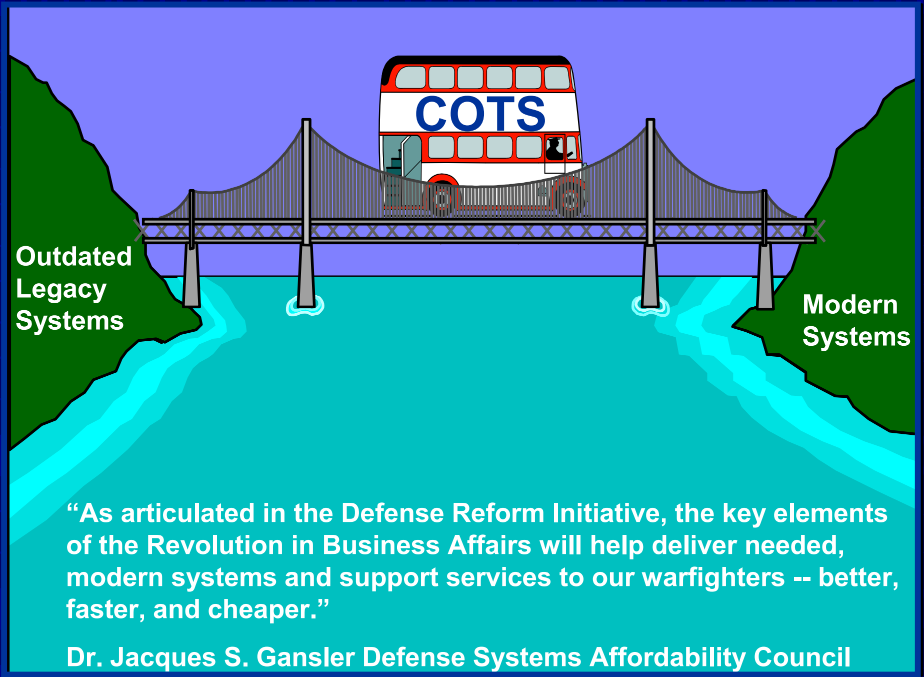
Why COTS?

➢Primary drivers:

- Cost
- Schedule
- Timely replacement of legacy systems
- Keeping pace with emerging technologies
- Lack of viable alternatives

How Did We Get Here?

Economic pressures and the much larger market place drive COTS products. The Government is no longer the leader or even a trendsetter in the market place. The Government has taken the position of Better, Faster, Cheaper and has identified COTS as the vehicle towards that end.



“As articulated in the Defense Reform Initiative, the key elements of the Revolution in Business Affairs will help deliver needed, modern systems and support services to our warfighters -- better, faster, and cheaper.”

Dr. Jacques S. Gansler Defense Systems Affordability Council

COTS Issues and Concerns

- Obsolescence
- Version Control
- Vendor support
- Testing Issues (regression testing)
- Robustness of Vendor’s testing is Unknown
- Inability to perform adequate structural coverage
- Maintenance
- Training

- Product Maturity
- Undisclosed Problems
- Absence of COTS Data (e.g., source code, test, validation, etc.)
- Vendor’s Development Process is Unknown
- Lack of knowledge in determining the best COTS product for your needs

NEW

- Security

Security Issues With COTS

- COTS products are inherently susceptible to intrusion
- COTS developers are:
  - Outside the control of the developing and contracting organizations!
  - COTS development personnel in all likelihood, do not possess a security clearance!
  - Many COTS products are developed in designated countries which may be sympathetic and possibly even supportive of terrorist organizations!
  - Outside organizations know more about your vulnerabilities than you do and can take advantage of them!
  - Time bombs can be placed within code that is virtually impossible to detect without the source code, etc. !

Safety’s Role

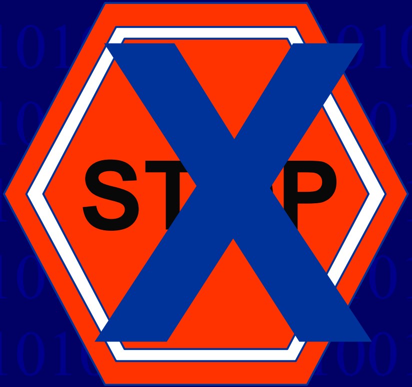
It is the safety community’s responsibility to take a proactive leadership role in mitigating the risk of COTS.

See, Hear, & Speak,

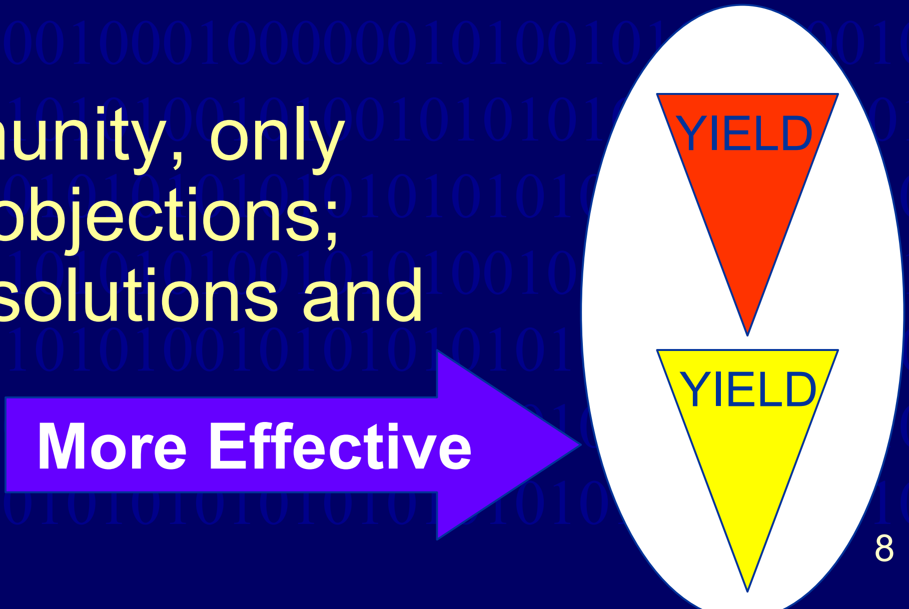
No Evil

Safety's Role

- ➢Safety cannot be perceived as a stop sign as program's will quickly learn to bypass safety to meet their objectives.



- ➢We cannot, as a community, only present concerns and objections; we must also suggest solutions and alternatives.



Issues Related to Integrating COTS Into Mission/Safety Critical Systems

John Covan

Airworthiness Assurance Department
Sandia National Laboratories
Albuquerque, NM

International System Safety Conference
September 12, 2001

Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company,
for the United States Department of Energy under contract DE-AC04-94AL85000.

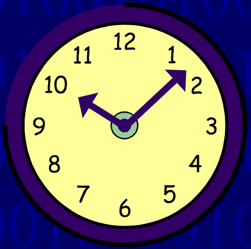
What is COTS?

- COTS: Commercial Off-the Shelf
  - a product designed & built to pre-existing, generic requirements
  - Could be hardware, could be software
  - Could be both

But why use COTS?

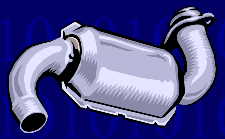
COTS Promises Up-Front Savings

- Faster
  - no development cycle
  - short lead time

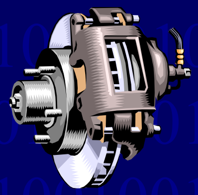


- Cheaper
  - Large quantity builds
  - R&D amortized over long time & many customers
  - Industry has lower overhead than for captive facility
    - cheaper labor
    - cheaper security costs

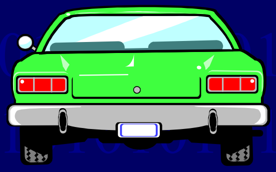
What Application of COTS?



- COTS piece-parts
  - Hardware
  - Software subroutine



- COTS subsystems
  - Hardware ensemble
  - Hardware/Software subsystem
- COTS turnkey system



All Types of Systems Are Threatened by Stressing Environments

Normal

- (occurs regularly)
  - operating environments (vibration, thermal cycling, aging)
  - inadvertent human error

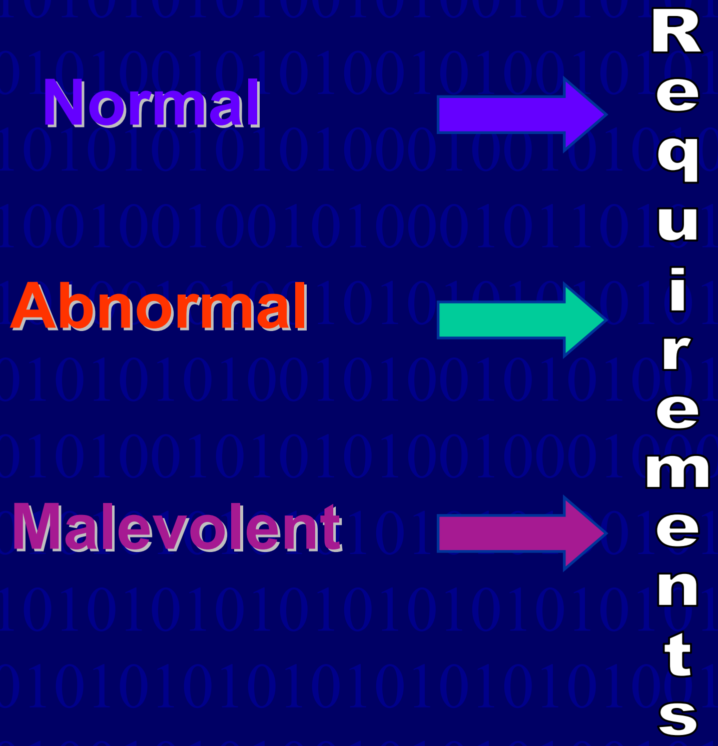
Abnormal

- (occurs at intervals)
  - accident environments (shock, crush, fire, immersion)
  - compounded by human error

Malevolent

- (occurs at intervals)
  - sabotage
  - outsider attack
  - insider attack

Stressing Environments Spawn Requirements



Normal

Abnormal

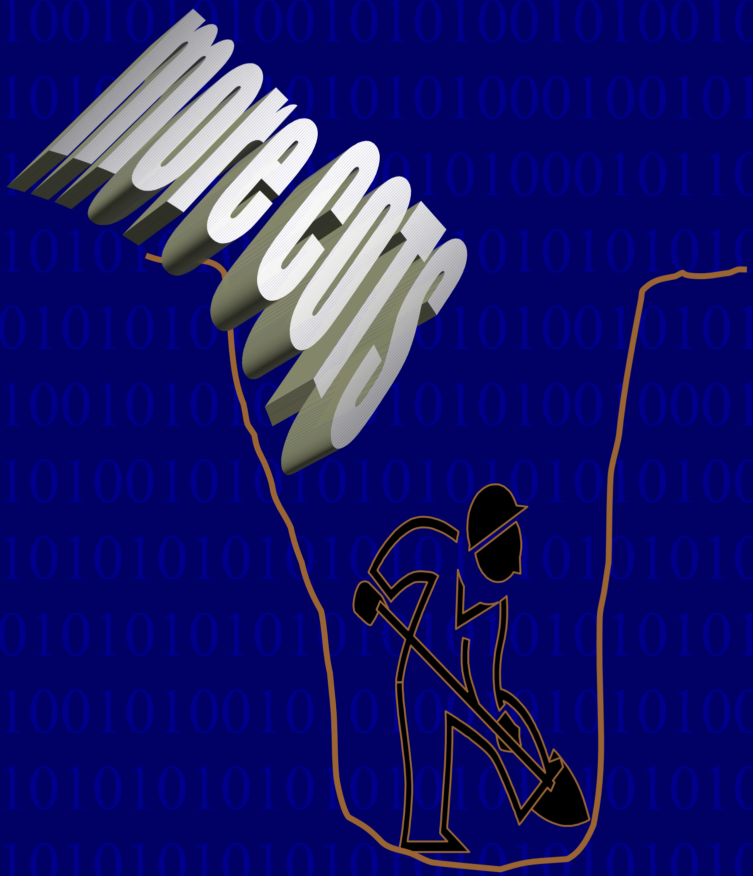
Malevolent

Requirements

What Do You Give Up With COTS?

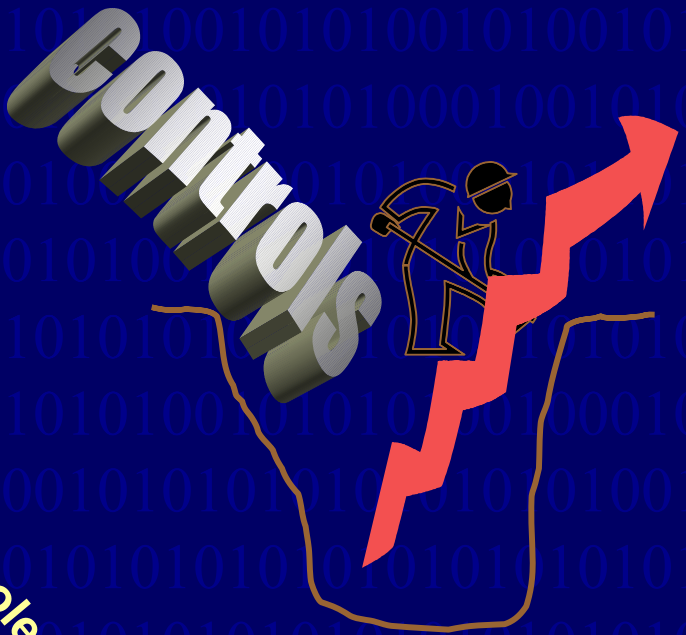
- Control
  - design may change over the product build to conform to availability of new materials or technology
  - product may vary from lot-to-lot by manufacture at a variety of facilities
- Information
  - You don’t know what went into it or who built it
  - You may not have access to source code

Does Using More and More COTS Cause Problems?



Digging yourself a hole…

And Are the Problems Surmountable?



Is climbing out of the hole feasible?

Climbing out of the hole…

Can this be done economically?

Some Retroactive Strategies

- Increased acceptance testing
- Blind buys
- Special build using screened employees

Problems With Retroactive Strategies

- ➢ Increased cost, increased schedule
  - From attempts to establish control that was not there in the first place
- ➢ Nagging doubts from incomplete information
  - Poor records of design, manufacture & installation
  - Proprietary information withheld
  - Source code withheld

Problems With Retroactive Strategies

- ➢ Strategies may be ineffective in the face of malevolence
  - – Vulnerabilities can include degraded materials, changes in dimensions, substituted parts, etc.
  - – Especially vulnerable when software is used *
    - Trojan horses
    - Time bombs
    - Logic bombs

*see *Why COTS Software Increases Security Risks*

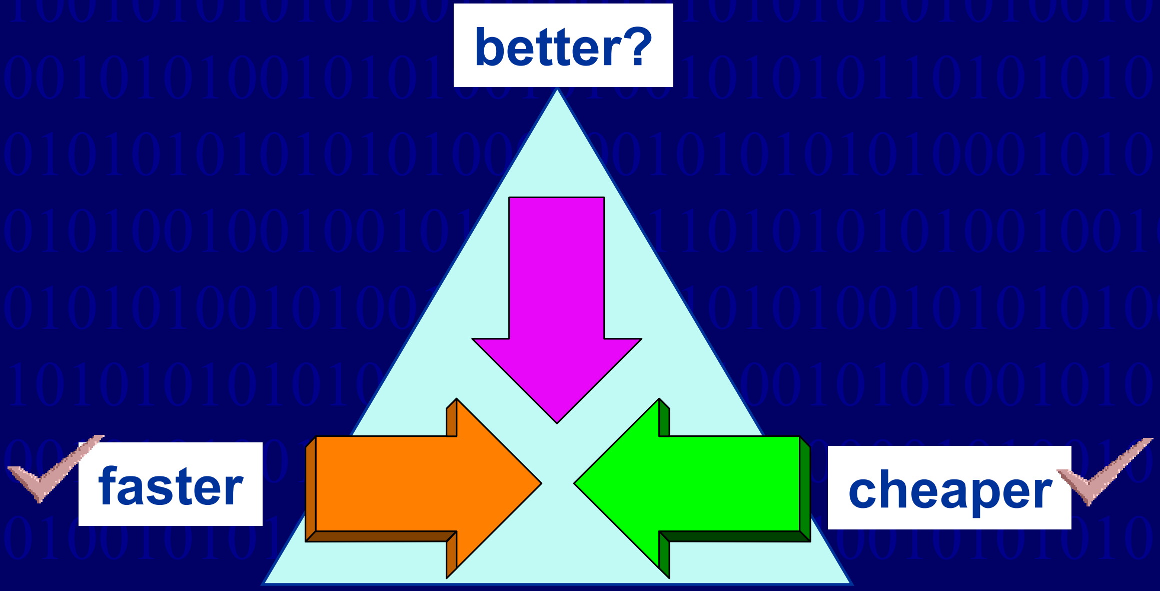
http://www.cigital.com/services/safety.html

Using COTS Implies Responsibility

Using COTS is **not** an excuse for

failing to meet system requirements

The Faster-Better-Cheaper Triangle

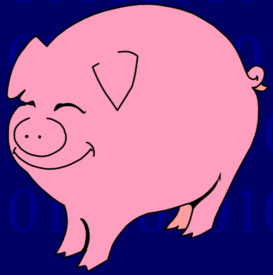


Buy now, pay later

More Cheap Shots...

- ➢If you want it bad, you'll get it bad

- ➢The best way to make a silk purse out of a sow's ear is to start with a silk sow



Is There a ‘Total Lack of Alternatives’ to COTS?

- No! Do surety-critical “fencing”…
- relegate surety-critical functions to small, walled-off portions of the system
  - develop, manufacture and install these functions in house
  - remainder of system can use some version of COTS

Ron Stroup

FAA AIO 200

Uma Ferrell

FAA Consulting

International System Safety Conference

September 12, 2001

SW Guidelines For CNS/ATM Systems- Background

- ➢RTCA SC 190 was chartered to document guidelines for CNS/ATM systems
- ➢Committee comprised of airborne community as well as ground community from US and Europe
  - – Cultural differences
  - – Domain differences
  - – Language (phraseology) differences
  - – Differences in the model for fielding a system

Domain Characteristics of CNS/ATM Systems

- ➢Very large systems compared to avionics
- ➢High use of COTS (telecommunications, for example)
- ➢Systems are acquired and commissioned for use in the ground infrastructure.
- ➢There are site differences in ground systems. The adaptation data is subject to verification.

Domain Characteristics of CNS/ATM Systems-2

- ➢Shadow operations for gaining confidence in the system as well as to train new controllers
- ➢24/7 use unlike airborne systems
  - – Continuous maintenance support
  - – Live insertion of updates
  - – Possibility of cumulative systemic errors

COTS and Safety in CNS/ATM Systems

- COTS received special attention in the document.
- Many issues documented in the guidelines were recognized to be business guidelines with safety effect.
- COTS acquisition model is considered within the CNS/ATM development model

COTS – a Part of the Bigger System

- ➢COTS Planning-within the context of the CNS/ATM system
- ➢Assessment and selection to form the basis of acquisition
- ➢Development of any “glue code”, partitioning, safety kernels, interface particular software
- ➢Verification
  - – No less than verification of developmental systems
  - – Within the context of the CNS/ATM system

Taking Advantage of the Domain Practices

- **Guarded use** of service experience for assurance credit to supplement other data
  - **Not applied at the highest level of safety**
  - **To be negotiated for the next lower level**
  - 8,760 service hours (one year) of continuous fault-free operation for the next lower level
  - 4,380 service hours (six months) of continuous fault-free operation for the next lower level
  - May not need use of service experience credit

Six assurance levels are defined for CNS/ATM systems

Service Experience Conditions

- Use this data only to supplement other data
  - Planning, Acquisition (assessment and selection) CM, QA
- Assure that data is collected during operations with real operational data, in relevant use, and in the same target environment.
- If the changes (HW/SW) are safety related, restart the clock.
- If the changes affect already collected data, restart the clock.

More Conditions to Enable Use of Service Experience

- Cover
  - All of the CNS/ATM needed functionality- analysis
  - All combinations of data input-analysis
  - All operational modes-analysis
- Analyze all service problems.
- Compute the service experience duration correctly noting that all safety-related problems restart the clock.
- Prove that unintended COTS capabilities do not affect CNS/ATM system operation.

Scrutiny to Assure Safety

- Safety Assessment – Establish level of assurance
- Life Cycle Data particular to COTS
  - Planning
  - Acquisition
    - Any developmental data
  - Verification Data
    - COTS testing and Integration testing
    - Time Duration-engineering judgment
    - Similarity of Operation/Environment
    - Problem Reporting
    - Analysis data
  - CM/QA within the context of CNS/ATM system
- Life Cycle data for any new SW (glue code)